The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE (S) ISSUED:
6/08/2012

SUBJECT:
Multiple Vulnerabilities in Adobe Flash Player Could Allow For Remote Code Execution(APSB12-14)

OVERVIEW:
Multiple vulnerabilities have been discovered in Adobe Flash Player that could allow attackers to take complete control of affected systems. Adobe Flash Player is a widely distributed multimedia and application player used to enhance the user experience when visiting web pages or reading email messages. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

SYSTEMS AFFECTED:
Adobe Flash Player 11.2.202.235 and earlier versions for Windows, Macintosh and Linux operating systems
Adobe Flash Player 11.1.111.9 and earlier versions for Android 3.x and 2.x
Adobe Flash Player 11.1.115.8 and earlier versions for Android 4.x, and
Adobe AIR 3.2.0.2070 and earlier versions for Windows, Macintosh and Android

RISK:
Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:
Adobe Flash Player is prone to six vulnerabilities that could allow for remote code execution and one unspecified security bypass vulnerability that could lead to information disclosure.

Two memory corruption vulnerabilities (CVE-2012-2034, CVE-2012-2037)

One stack overflow vulnerability (CVE-2012-2035)

One integer overflow vulnerability (CVE-2012-2036)

One security bypass vulnerability (CVE-2012-2038)

One null dereference vulnerability (CVE-2012-2039)

One binary planting vulnerability (CVE-2012-2040)

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Failed exploit attempts will likely result in denial-of-service conditions.
Flash Player installed with Google Chrome will be updated automatically, so no user action is required. Google Chrome users can verify that they have updated to Google Chrome version 19.0.1084.56, which includes Adobe Flash Player 11.3.300.257.

RECOMMENDATIONS:

The following actions should be taken:

- Users of Adobe Flash Player 11.2.202.235 and earlier versions for Windows and Macintosh should update to Adobe Flash Player 11.3.300.257.
- Users of Adobe Flash Player 11.2.202.235 and earlier versions for Linux should update to Adobe Flash Player 11.2.202.236.
- Users of Adobe Flash Player 11.1.115.8 and earlier versions on Android 4.x devices should update to Adobe Flash Player 11.1.115.9.
- Users of Adobe Flash Player 11.1.111.9 and earlier versions for Android 3.x and earlier versions should update to Flash Player 11.1.111.10.
- Users of Adobe AIR 3.2.0.2070 for Windows, Macintosh and Android should update to Adobe AIR 3.3.0.3610.

Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

Remind users not to download or open files from un-trusted websites.

Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.

Remind users not to click links from unknown sources, or to click links without verifying the intended destination. Consider implementing file extension whitelists for allowed e-mail attachments.

REFERENCES:

Adobe:

http://www.adobe.com/support/security/bulletins/apsb12-14.html
http://blogs.adobe.com/psirt/2012/06/security-updates-available-for-adobe-flash-player-apsb12-14.html

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2034
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2035
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2036
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2037
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2038
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2039
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2040